TRIBE

Insight Paper:

BUILDING A CYBERSECURE CULTURE

Engaging employees in personal responsibility

TABLE OF CONTENTS

Section 1

INTRODUCTION

Tribe's perspective

TRIBE'S PERSPECTIVE

We have the benefit of an outsider's view, because we've seen behind the curtain in so many organizations. We've worked with the employee audience for over 20 years, starting in 2002 with Porsche and UPS.

Since 2009, we've focused our practice exclusively on the employee audience. Over the years, we've worked with some of the world's largest companies and most well-known brands, from Amazon to Cargill and Levi's to Coke.

We're not experts in cybersecurity; our expertise is in shifting employee behavior and building culture through effective communications. In the practice area of cybersecurity, we've built engagement with employees in both office and manufacturing settings, and in global locations from South America to South Asia.

This insight paper shares some of the learning we've gained over our decades of experience. We hope it offers you an idea or two, or maybe a new way of approaching your cybersecurity communications for employees.

We've worked with some of the world's largest companies and most well-known brands, from Amazon to Cargill and Levi's to Coke.

Section 2

THE HUMAN LIMITS OF CYBERSECURITY

No technology you can buy can eliminate employee error

CYBERSAFE CULTURE

No doubt you've invested significantly in platforms and tools to maintain your company's cybersecurity. But unfortunately, there's no technology you can buy that completely protects against the possibility of an employee clicking on something they shouldn't.

That's why it's so important to build a culture of cybersecurity, so that employees feel a personal responsibility for keeping the company safe. Successfully engaging employees in a cybersafe culture extends beyond just an awareness of evolving phishing schemes and physical breaches. It helps create a security mindset so that employees approach all aspects of their job with mindfulness — whether they're developing software or managing supply chain operations.

Compliance training, phishing tests and educational materials from Mimecast, KnowBe4, SANS, Hoxhunt or whatever platform you've invested in are an essential first step. But those tools stop short of making cybersecurity a cultural concern.

Help employees feel a personal responsibility for keeping the company safe by building a culture of cybersecurity.

Not just an IT issue

Cybersecurity requires the dedication of employees throughout your organization, not just those who work in IT. This means positioning cybersecurity as an ongoing conversation inside the company. It means involving leaders throughout the company to make the message personal to their teams. And featuring employees and managers as influencers for their peers.

Let executive leadership set expectations

By involving executives across the C-suite, you'll be able to engage employees in your entire range of departments and job functions.

When the head of operations speaks to cybersecurity concerns in manufacturing facilities, retail locations or labs, those employees will take the concerns more seriously than they might otherwise. When the CFO addresses invoice scams and other financial hacks, his or her people will pay attention. The message to employees becomes clear: Each one of us is responsible for the company's cybersecurity.

Employees are influenced by each other

In the same way that consumers depend on customer reviews for their purchasing decisions, employees pay attention to what their peers have to say about cultural issues. When you use managers and employees as influencers to emphasize the importance of and best practices for cybersecurity, you're able to engage employees in a more personal way.

Branding your educational materials.

Your cybersecurity employee platform is a source of rich content, but whether you use Mimecast, KnowBe4, SANS, Hoxhunt or another, it all looks like generic material from an outside vendor. By customizing their materials with your company branding, you send a subtle but important message: This is a conversation that's happening inside the company.

The message to employees becomes clear: Each one of us is responsible for the company's cybersecurity.

Section 3

MAKING IT EVERYONE'S RESPONSIBILITY

Elevating cybersecurity awareness to equal workplace safety

BACKGROUND

Avery Dennison is a global manufacturer with valuable IP, including proprietary technologies and customer formulations. Citing the growing (and ever-changing) risks of cybersecurity, one of the board members recommended the company develop a strategic communications approach to engaging employees in their personal responsibility for cybersafety.

Workplace safety was already a point of cultural pride. Employees are highly aware of their responsibilities for keeping themselves and each other physically safe.

This strategic communications plan would be directed at engaging over 35,000 employees, in both office settings and manufacturing facilities, located in more than 50 countries around the world. Materials would need to be translated into at least eight languages.

THE CHALLENGE:
Make cybersecurity equal to workplace safety

Our goal was to inspire employees to treat cybersecurity with the same level of caution and accountability as they do physical safety.

This strategic communications plan would be directed to over 35,000 employees, in both office settings and manufacturing facilities.

DISCOVERY

Stakeholder interviews and employee audience matrix

The goal of our Discovery process is to identify the gap between leadership's vision and the workplace reality. Our communications strategy addresses how to close that gap.

Tribe interviewed nine executive leaders and key members of their teams. These leaders included the CTO, CFO, EH&S manager and top executives of the Materials group and the Solutions group.

Stakeholder interviews indicated a significant concern with the difficulties of creating a sense of personal responsibility for cybersecurity. They felt an urgency about building an ownership mindset around keeping the company cybersecure.

These conversations also reinforced our perception of cybersecurity as equal to, or perhaps an element of, physical workplace safety. Because workplace safety is already a central theme in their culture, they saw the possibilities for creating a cultural bias for cybersecurity as well.

Audience matrix

The workforce is organized by business unit and global region, with locations in 44 countries. Like most manufacturing companies, the majority of their employees are in operations roles.

Stakeholders felt an urgent need to develop a sense of personal responsibility for cybersecurity.

Analysis of employee risk

- **Every employee represents a potential point of failure**
  Threat actors can break into an organization through just one employee, which means every single employee is a target.

- **Different employee audiences present different risks**
  For instance, employees in factories might be targeted to shut down manufacturing systems, while wired employees are targeted for invoice fraud.

- **Low awareness of business impact**
  Although cyberattacks could cost the company losses in the tens of millions of dollars, employees often treated these threats as low-level distractions in their day-to-day jobs.

THE GAP:

Our goal was to elevate employees' ownership of cybersecurity to the level of responsibility they already felt for physical safety in the workplace.

STRATEGY

Put the onus on individual employees

Use a branded, yearlong, multichannel campaign to reach all employee audiences.

Steps and tactics:

- One rallying cry that speaks personally to employees
- Use executive leadership to own the messaging
- Make influencers of employees and managers
- Apply Avery Dennison branding to Mimecast materials

These communications were organized by monthly themes, so that we could break the messaging down into digestible elements — and communicate a comprehensive inventory of messages over the year.

RALLYING CRY

The campaign theme that unites all cybersecurity communications

Reinforces the notion that every single employee is accountable for cybersecurity and celebrate that role rather than pointing fingers. This is not an abstract concern but a personal responsibility. The mark also incorporates the Avery Dennison triangle brand symbol.

STEAL THIS INSIGHT:

To make an emotional connection with employees and move them to shift their behavior, craft your cybersecurity communications to speak human to human — rather than leaning on technology language and abstract visuals.

LEADERSHIP PODCASTS

Using executive leadership to start the conversation from the very top

These podcasts were also excerpted and repurposed as articles on the intranet page devoted to cybersecurity. We find that leadership podcasts are a popular channel for employees, particularly desk employees who sometimes play them as they work.

"One of our strongest values as a manufacturing organization is that we keep each other safe. And I think taking the same approach to cybersecurity is a fundamental requirement."

Deon Stander
Chief Executive Officer

"So what can leaders do to help keep us cybersafe? It starts with driving home the importance of cybersecurity with your teams. Your influence really matters."

Nick Colisto
Chief Information Officer

"Should our information be accessed, one of the worst things that would happen is a breakdown of trust between us and our customers."

Ryan Yost
President, Materials Group

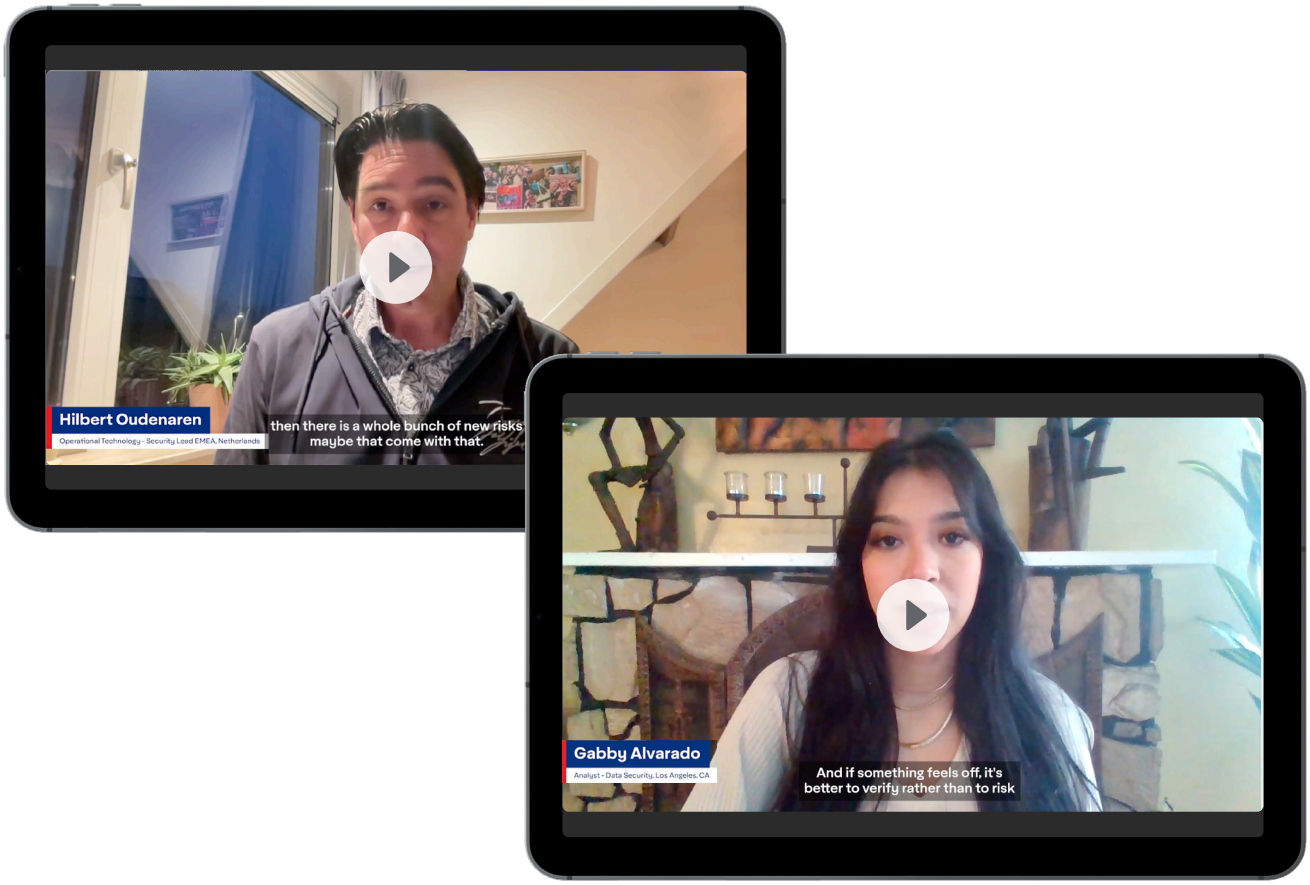
STEAL THIS INSIGHT:

Podcasts give an opportunity for a deeper dive into complex topics and are particularly well-suited for executive communications. They also create a Fireside Chat-like sense of human connection between employees and the company leadership.

VIDEOS

Driving deeper into the organization to enable employees to influence each other

These videos were shot remotely and edited at Tribe for a cost-efficient solution that enabled us to show the faces of employees throughout the company. Subtitles make them appropriate for digital monitors in manufacturing facilities, as well as in the break areas of office locations. The pandemic changed the world's acceptance for remote videos, which are now used by most major news outlets.



STEAL THIS INSIGHT:

Just like consumers rely on customer reviews, employees relate to what their peers have to say on a topic — and often identify with their challenges and solutions.

MANAGER TOOLKITS

Helping managers engage their teams with manageable messaging

Each monthly theme is covered in a conversational guide that gives both a high-level summary and deep dive with more details. These materials are equally appropriate for meeting rooms in offices and pre-shift meetings in manufacturing facilities.

Manager toolkit

Phishing

When you don't know what's at stake, talking with your employees about cybersecurity might feel daunting or unengaging. But cybersecurity is a big deal, and each of our employees plays a crucial role in keeping us safe. Use this info, especially the talking points, in your huddles and discussions with your teams.

Reporting concerns

If you manage employees with an email account and/or ad:a credentials, they should report suspicious activity or cybersecurity incidents via:

- Email securityoperations@averydennison.com
- Use the Report a Security Incident link at the bottom of the home screen.

If you manage employees without an email account and/or ad:a credentials, they should report suspicious activity or cybersecurity incidents to you or the local GTS contact.

YOU'RE THE ONE
KEEPING US CYBERSAFE

What is phishing?

Phishing is the most common type of attack we experience at Avery Dennison.

Three common ways to spot a phishing attack are misspelled words and poor grammar, suspicious links or attachments and a false sense of urgency. But these aren't the only ways. Attackers today are evolving and often do a good job impersonating people we know or who work for Avery Dennison, and it takes careful consideration to notice when they're asking for information that shouldn't be shared.

Other things to look out for:

- unsolicited emails, phone calls, SMS, or social media messages requesting information or action.
- The use of official Avery Dennison banners and logos
- Sales promotions and other non-work offers that seem too good to be true

Remember: When in doubt, report messages as phishing using the Report Phishing button.

How we prepare

Why we send phishing exercises

Research has shown that falling for a cyber criminal's trick is the most effective way to improve your cybersecurity habits. In support of our company's data protection efforts, the IT Security team sends employees simulated phishing emails that resemble common attacks being used by hackers. While these are only tests to educate you on the heightened risks, if these were real, company and personal information could be compromised. While these emails can be embarrassing, they're a great opportunity to consider our habits and learn to be more cautious.

Educating our employees to use sound judgement

Ensuring employees know how to spot phishing attempts is extremely important. Educational content is regularly posted to the cybersafety page on OurWorld, and short training modules are shared frequently to show employees how to use Sound Judgement to avoid Human error.

You're the One

At Avery Dennison, we've created a strong foundation for information protection, but our approximately 35,000 employees are the first line of defense and our biggest vulnerability to attackers.

Your decisions and actions each day can significantly impact our collective efforts. Our global cybersafety program, You're the One, is designed to help every employee:

- Understand the importance of building a cybersafe culture - and what's at stake if we don't.
- Practice sound judgement to avoid human error in their daily work.
- Know how to spot and report suspicious activity or incidents.

AVERY DENNISON MAKING POSSIBLE™

Manager toolkit

Data in motion

When you don't know what's at stake, talking with your employees about cybersecurity might feel daunting or unengaging. But cybersecurity is a big deal, and each of our employees plays a crucial role in keeping us safe. Use this info, especially the talking points, in your huddles and discussions with your teams.

Reporting concerns

If you manage employees with an email account and/or ad:a credentials, they should report suspicious activity or cybersecurity incidents via:

- Email securityoperations@averydennison.com
- Use the Report a Security Incident link at the bottom of the home screen.

If you manage employees without an email account and/or ad:a credentials, they should report suspicious activity or cybersecurity incidents to you or the local GTS contact.

YOU'RE THE ONE
KEEPING US CYBERSAFE

What is data in motion

When we talk about data in motion, we're referring to all the ways we store and share digital data.

That can involve USB or flash drives, cloud storage, hard drives, and more. Cyber criminals have all sorts of tricks to get into our systems or steal our data related to the ways we're storing and sharing things digitally.

Three common threats to our data are infected USBs, physical site breaches, and infiltration through Google Drive or other cloud storage.

Cyber criminals have lots of ways to get infected USBs into seemingly secure sites. Sometimes they'll leave USB drives laying around, waiting for someone to pick them up and use them. Another clever tactic is to infect a phone or other personal device, and wait for that device to have a USB connection to a secure Avery Dennison system. Sometimes scammers will even manufacture cheap USB-powered devices, and sell them without charging blocks, encouraging users to plug them into valuable systems with USB ports, giving them an opportunity to get access.

Physical site breaches are another way cybercriminals try to get access to our data. If a criminal can get their hands on one of our devices, they have a better chance of getting into our networks. Only let approved guests into our sites, and never let them leave your site once they're in. If you see someone who doesn't work with us in one of our facilities unaccompanied by an employee, report it to me immediately.

How we prepare

USB drive scanners

To avoid data threats from infected or unknown USBs, use a secure USB drive scanner before plugging a USB drive into an Avery Dennison system, and never plug your phone into an operational machine.

Education

Ensuring employees know how to spot potentially risky environments is very important. Educational content is regularly posted to the cybersafety page on OurWorld, and short training modules are shared frequently to show employees how to use Sound Judgement to avoid Human error.

You're the One

At Avery Dennison, we've created a strong foundation for information protection, but our approximately 35,000 employees are the first line of defense and our biggest vulnerability to attackers.

Your decisions and actions each day can significantly impact our collective efforts. Our global cybersafety program, You're the One, is designed to help every employee:

- Understand the importance of building a cybersafe culture - and what's at stake if we don't.
- Practice sound judgement to avoid human error in their daily work.
- Know how to spot and report suspicious activity or incidents.

AVERY DENNISON MAKING POSSIBLE™

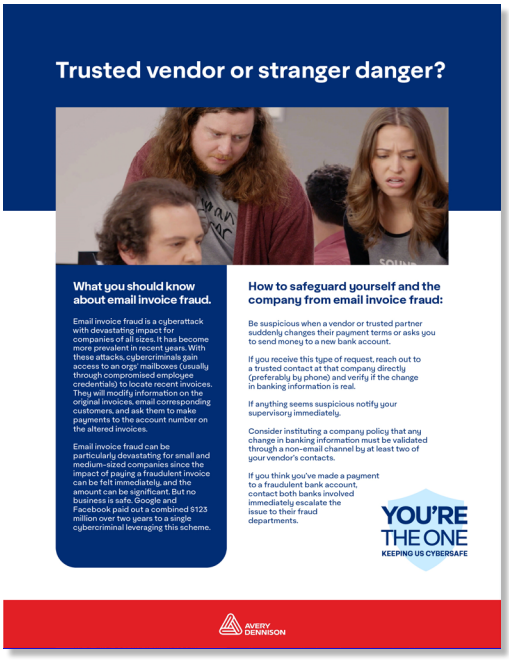
STEAL THIS INSIGHT:

Most managers are not trained communicators. If you're asking them to share your messaging, give them the tools to make the job as easy as possible for them.

MIMECAST MATERIALS

Customizing existing materials with Avery Dennison branding

Avery Dennison had access to an extensive library of content in their Mimecast platform, which we branded with the You're the One campaign to tie it back to our internal cybersecurity conversation.



STEAL THIS INSIGHT:

Use what you've got. Instead of recreating new educational materials, take advantage of those resources your cybersecurity platform provides — but customize them with your branded cybersecurity campaign.

ENVIRONMENTAL SIGNAGE

Using creative touchpoints in the workplace

If it's digital, it's sometimes invisible. We supplemented the many online materials with physical reminders in the workplace, from zero-trust USB kiosks to digital monitors to restroom mirrors.

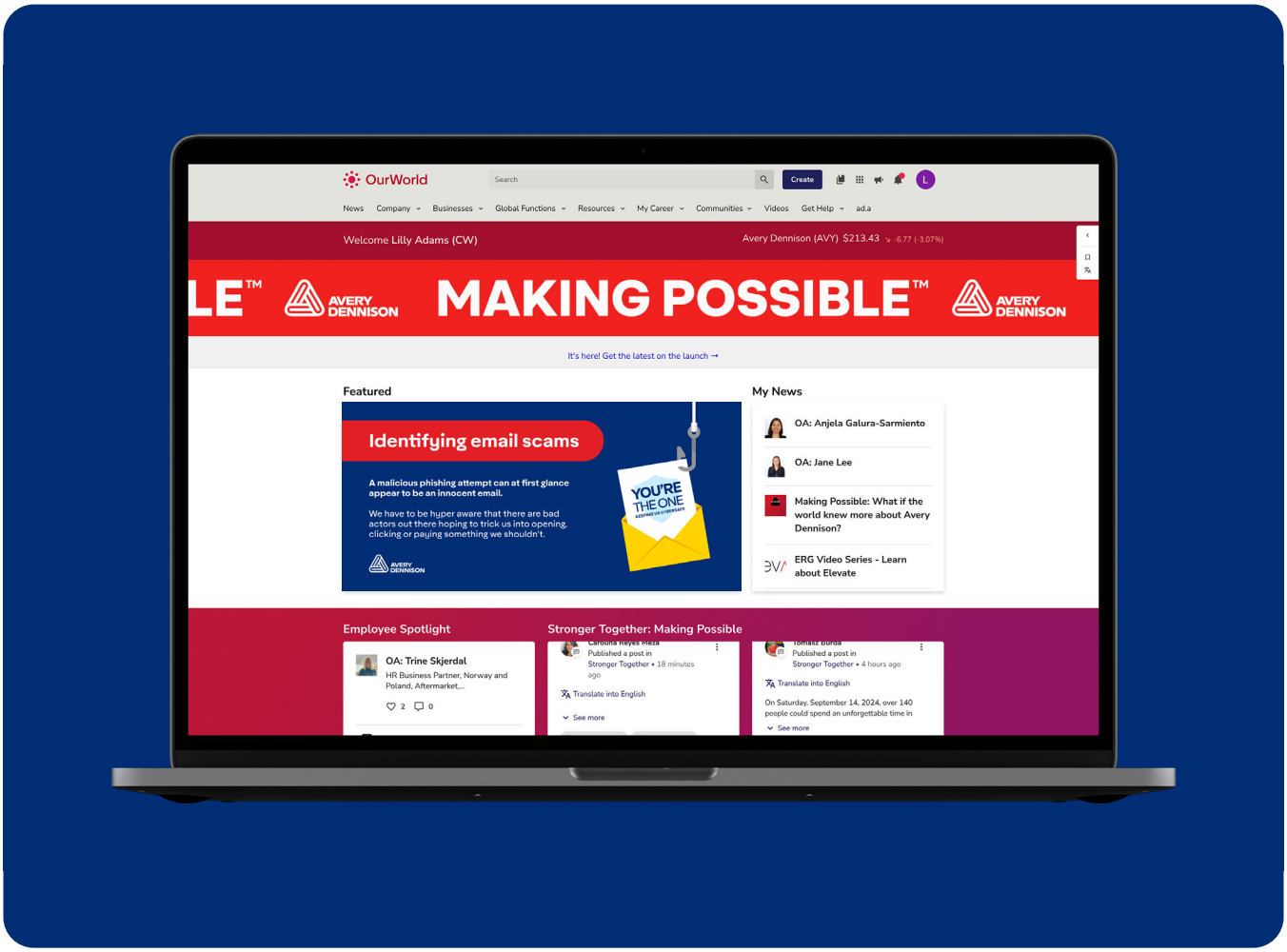
STEAL THIS INSIGHT:

Go to the worksites. Particularly when dealing with non-desk audiences like manufacturing employees, it's helpful to see the physical realities of their workplaces. That's how you'll discover unexpected touchpoints that can be particularly effective.

INTRANET PAGE

Creating a home for all materials related to the cybersecurity campaign

An existing page on the intranet was updated with You're the One campaign branding and the current content for the monthly team. Archives of campaign materials are easily searchable.



STEAL THIS INSIGHT:

Make it easy for employees and managers to find these materials with a go-to online resource. Use other channels, particularly those like digital signage that offer limited copy space, to direct people here for more information.

RESULTS

Award-winning campaign

2025 CSO50
Award Winner

The campaign was launched in January of 2025, so results will be measured at the beginning of 2026. But Avery Dennison has already received industry recognition. The You're the One campaign was among the CSO50 award winners for 2025.

Section 4

5 TAKEAWAYS

Parting thoughts from Tribe's experience

1

Commit to communicating over the long term

It's not possible to make a company-wide shift toward personal responsibility for cybersecurity without sustained communications over a year — or more. Keep those cybersecurity communications coming in a steady flow.

2

Start at the top and then equip managers below

Having your C-suite lead the way for heightened awareness of cybersecurity lets employees know this is serious. But they'll depend on their managers for more detail, so make it easy for managers to engage and influence them on the topic.

3

Leverage a mix of media and channels

When communicating with employees, consider the different work environments, as well as cultural or geographical differences, and even generational preferences in media consumption. Include online articles, videos, podcasts, digital signage and environmental signage. Use both short messaging and some longer copy for more complex topics.

4

Speak human to human

Even though you're talking about technology — and creepy technical things like malware — let your communications speak conversationally. Appeal to employees on a personal level.

5

Remember they don't have to pay attention

Employees don't have to consume any of the communications we offer them. That's why it's so important to offer a variety of channels, and to use a high level of creativity in your communications.

Section 5

WHY TRIBE?

When considering support from an agency

If you're considering agency support, either for an isolated project or over the long term, we hope you'll consider Tribe.

We're a tiny global agency that's worked with some of the largest and most well-known brands in the world.

Our practice is entirely focused on internal communications. If it's a communications challenge related to the employee audience, we've probably seen it before.

Our size makes us agile and responsive, so we can respond quickly and work comfortably on tight deadlines.

We're familiar with employee audiences in an expansive range of industries including manufacturing, technology, healthcare, retail, hospitality, construction, finance and energy.

Section 6

REFERENCES

What our clients say

We're happy to connect you with Tribe clients whose communications challenges or industries match yours, but in the meantime, here are a few comments from client partners.

"We've never had a better agency experience. Tribe has been a true pleasure to work with."

Justin Downs
Group Vice President, Operations, Wabtec Corporation

"Working with Tribe was like flipping a light switch for us — suddenly, our mission, vision and values weren't just words on a wall, they became something our teams could actually see themselves in. They have a knack for pulling the DNA out of a company and turning it into something meaningful and actionable. The process was thoughtful, collaborative and, honestly, a lot of fun. I'd work with them again in a heartbeat."

Lauralee Heckman
Director of Communications, The Lane Construction Corporation

"Tribe has been super easy to work with. They've been a great thought partner, and great at execution, which is clearly important as well. I feel Tribe is a part of Orveon. They know us better than any other organization that's not internal."

Robert Rigby-Hall,
Chief People Officer, Orveon

"Tribe's creativity in developing a comprehensive, yearlong, multimedia campaign was instrumental in bringing our vision to life. The collaboration was seamless, and your ability to customize our content and involve our employees made the messaging feel authentic and impactful. It was a pleasure working with such a smart, responsive and talented group of people."

Jeremy Smith
VP and Global Information Security Officer, Avery Dennison

"Tribe has been an integral part of building our culture. Their plethora of expertise and knowledge makes working with them so easy. Tribe really gets it and produces great ideas and results."

Paula Lamoureux
Global Internal Communications Manager, Ensono

"Tribe has been a trusted and valuable partner to us over the past several years on multiple tough-to-tackle projects. They have always taken the time to truly understand our corporate culture and our brand so that the solutions they provide are authentic to us."

Chrissy Hughes
Senior Brand Manager, Holder Construction

TRIBE

Tribe, Inc.
2100 Riveredge Pkwy
Suite 720
Atlanta, GA 30328
404-256-5858
tribeinc.com

Elizabeth Cogswell Baskin
CEO, Executive Creative Director
elizabeth@tribeinc.com

Steve Baskin
President, Chief Strategy Officer
steve@tribeinc.com